Cascading failure in the topological model

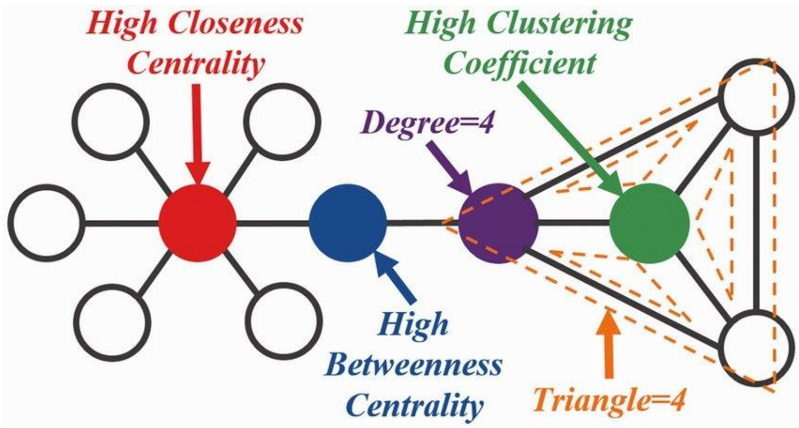
In power grids when one of the elements fails (completely or partially) and shifts its load to nearby elements in the system. Those nearby elements are then pushed beyond their capacity, so they become overloaded and shift their load onto other elements. [8]

Cascading failures are the consequence of the collective dynamics of the complex power grid. Large scale cascades are typically due to propagation of a local failure into the global network.[7]

Topological models

Any graph or network has two basic components – nodes and edges. An unweighted network can be represented as an adjacency matrix (A). Any element of adjacency matrix (A) a_{ij} , is given as

$$a_{ij} \begin{cases} 1, & \text{if } i \neq j \text{ and i and j nodes are connected by edge} \\ 0, & \text{if } i \neq j \text{ and i and j nodes are not connected} \\ 0, & \text{if } i = j \end{cases}$$



- Node Degrees distribution（度中心性）

  Defined as the number of links incident upon a node. The degree of any node i is represented by:

$$k_i = \sum_j a_{ij}$$

  The probability of degree distribution is represented by

$$P(k) = \frac{N(k)}{\sum N(k)}$$

  where N(k) is the number of nodes in the network with degree k.

  The average degree of a network is given by

$$< k > = \frac{\sum_i k_i}{N}$$

where N the total number of nodes in the network.
Higher degree of a node implies stronger connectivity of the node in the network.

- Closeness Centrality (接近中心性)

The proximity between one node and other nodes in the network. Calculated as the reciprocal of the sum of the length of the shortest paths between the node and all other nodes in the graph. Thus, the more central a node is, the closer it is to all other nodes.

$$C(x) = \frac{1}{\sum_y d(y,x)}$$

Where d (y, x) is the distance between node x and y.

- Betweenness Centrality (中介中心性/中间中心性)

A measure of centrality in a graph based on shortest paths.

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

Where σ_{st} is total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths that pass through v.

- Characteristic path length of a network

The characteristic path length (L) of a network is the shortest path length between two nodes averaged over all pairs of nodes and is given by

$$L = \frac{\sum_i \sum_j L_{i,j}}{N(N-1)}$$

Where $L_{i,j}$ is the shortest path length between i^{th} node and j^{th} node.
Higher characteristic path length implies network is almost in liner chain and lower characteristic path length shows the network is in compact form.

- Clustering coefficient of a network

The clustering coefficient (C) is a measure of local cohesiveness. Traditionally the clustering coefficient C_i of a node i is the ratio between the total number (e_i) of the edges actually connecting its nearest neighbors to the i^{th} node and the total number of all possible edges between all these nearest neighbors [$\frac{k_i(k_i-1)}{2}$; if the i^{th} vertex has k_i neighbors] and is given by

$$C_i = \frac{2e_i}{k_i(k_i-1)}$$

where e_i is the total number of edges actually connecting the i^{th} node's nearest neighbors. Then the clustering coefficient of a network is the average of its all individual C_i 's.
The average clustering coefficient of a network is given by

$$< C > = \frac{\sum_i C_i}{N}$$

Here, N is the total number of nodes of the network.

Robustness and vulnerability analysis

Many approaches analyze the robustness and vulnerability of power system by removing components from the system and evaluate the impact under different removing strategies. Some studies are using Monte Carlo method to simulate all possible contingencies so that the most likely failed components can be obtained [5, 8,17-18]. Recently [13], presented a network-based Markov chain model to study the propagation dynamics of the entire power networks. Robustness of the power network has been analyzed through the model. Robustness has been analyzed using the model that is derived from admittance model with two new robustness metrics percentage of unserved nodes (PUN) and percentage of noncritical links (PNL) introduced [14]. Fig. 1 illustrates the structural topology of power networks of the IEEE 118-bus test system with decentralized generator location in (a) and a centralized one in (b), where red squares represents the generators [14]. The result showed that for a given number (percentage) of available generators in a power system, the decentralized generator locations may greatly increase the robustness of the power grid.[16] summarizes concepts about its technical definitions and references therein can be found in figure2.

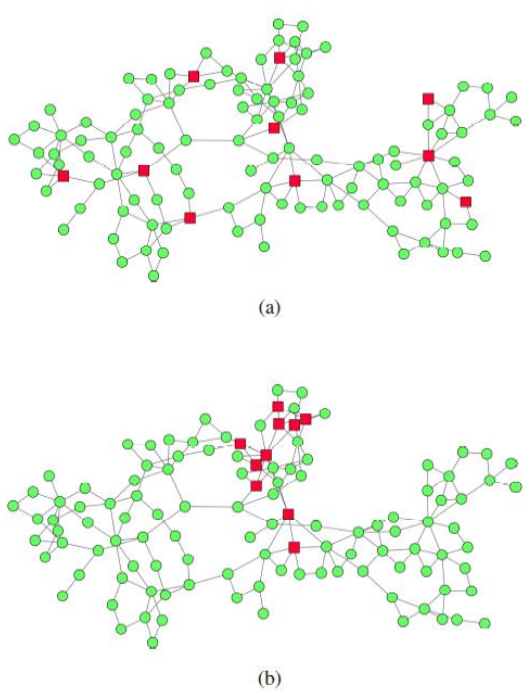


Figure 1 The figure illustrates the topology of power networks. (a) IEEE 118-bus with

Concept	Definition	Ref.
Reliability	Probability that an electric power grid can perform a required function under given conditions for a given time interval (IEC definition). The probability of its satisfactory operation over the long run (IEEE definition).	[45] [48]
Disturbance	An unexpected event that produces an anomalous system condition.	[45]
Contingency	The unexpected failure or outage of a network component, such as a generator, transmission line, or other electrical element.	[45]
Robustness	Degree to which a network is able to withstand an *unexpected* event without degradation in performance. It quantifies how much damage occurs as a consequence of such unexpected perturbation.	[49]
Vulnerability	The lack of robustness. Vulnerability is often used to score low reliability of power grids. It can be quantitatively defined by Equation (1).	[12]
Resilience	The ability of a power system to recover quickly after a disaster or, more generally, the ability of anticipating to extraordinary, high-impact, low-probability events, quickly recovering from these disruptive events, and adapting its operation and structure for preventing or mitigating the impact of similar events in the future.	[45]
Resilience *vs.* robustness	Robustness measures *how much* damage occurs as a consequence of an unexpected perturbation, while resilience measures *how quickly* the network can retrieve from such damage.	[49]
Resilience *vs.* reliability	Resilience is related to *low probability*, *high impact* events. It is a dynamic concept. Reliability is related to *high probability*, *low impact* events. It is a static concept.	[41,49]
Stability	The ability to maintain or to recover a state of equilibrium after disturbances or contingencies.	[40]
Critical Infrastructure	Infrastructure whose unavailability or destruction would have a extensive impact on economy, Government services and, in general, on everyday life, with severe consequences for a nation. Examples of critical infrastructures are power grids, telecommunication networks, transportation networks, water supply systems and natural gas and oil pipelines.	[50–53]

Figure 2 Summary of definitions related to robustness in power grids and their references.

Strategies to Improve Robustness[16]

1. Intentional Islanding

Intentional islanding is a strategy to stop the initial failure occurring in a small part of a power grid, and to prevent it from propagating through the rest of the system causing thus a larger blackout.

2. Smart Addition of Links

The first one is that networks with small diameter are very robust. This has very important practical implications because from a practical engineering viewpoint, it involves that generators should be placed near consumers, which can be attained by means of distributed renewable energy generation. The second important conclusion is that networks can be made typically more robust by adding more links.

3. Hybrid Power Grids.

The term “hybrid” is interpreted by the authors in two distinct yet related ways: the combination of actions to increase the infrastructure robustness (new lines) along with smart operational actions; and the coexistence of largely interconnected grids with central control and smaller, decentralized areas that could be operated as “microgrids” in case of emergency.

4. Smart Grids

The exchange of electric energy at a local level could be very positive because it would stimulate the local production and consumption of renewable energy (e.g., small-scale photovoltaic panels and wind turbines), hence aiding the end-user to obtain economic benefits by selling the energy produced in excess, and making the power grid more robust.

Mitigation and prevention of cascading

Mitigation approach aims at reducing the impact of cascading failure by load shedding, line switching or some other remedial actions. Prevention of the cascading utilizes some fast response remedial actions at each stage of the cascading to prevent or at least mitigate the spread of the cascading. [4] present the effect of topology in determining the robustness of a power grid. Three mitigation strategies, Homogeneous Load Reduction, Targeted Range-Based Load Reduction, and Use of Distributed Renewable Sources in combination with Islanding. The comparison method are Characteristics path length and clustering coefficient.

Dynamical model

[1] Use a dynamical model of cascading failures to evaluate the relation between the size and scope of blackouts due to node failures and the level of load of the network relatively to its capacity, which may be thought of as a measure of the proximity of the system state to its operational limit. Recent models have involved timescale of dynamic during the cascading [12,15]. Following the methodology proposed in [2], the efficiency of a path is modeled as the harmonic composition of the link it goes along, such that the average efficiency of the network

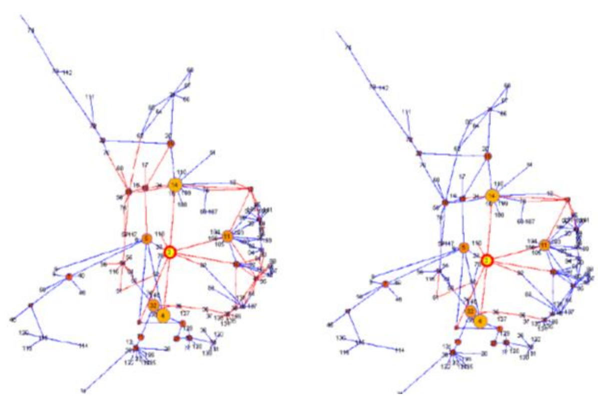


Figure 3 (left) Cascading failure due to the removal of the node with highest load(node 3. Circled with red line) for n = 1.5:38.33% of the transmission line are tripped offline (in red) (right) Cascading failure due to the removal of the node with highest load(node 3. Circled with red line) for n = 2.6.5:13.89% of the transmission line are tripped offline (in red)

Result : same topological structure can behave quite differently to individual failures, depending on the spare capacity of the remaining nodes and links.

Complex network perspective

From a complex network point of view, a power grid can be simply demonstrated by a graph, where nodes or vertexes represent generators, transformers or loads, and links or edges represent transmission lines. Based on this structure, many different intrinsic characteristics have been applied to

nodes and edges, in order to better reveal electrical properties in the power grid [9,2]. Studies focused on different countries got the similar conclusion that the power network belongs to small-world networks [19]. A survey of studying complex network theory for modern smart grid applications has been proposed in [10].

Other Method

[3] proposes a novel ICI algorithm based on a Linear Programming (LP) formulation that directly determines an islanding solution with minimal power-flow disruption for any given number of islands, while ensuring that each island contains only coherent generators. To improve time execution and effectiveness

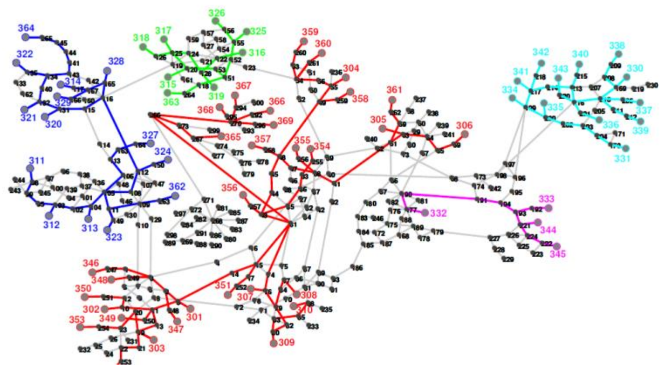


Figure 4 SSR result on IEEE 300-bus test system for K = 5

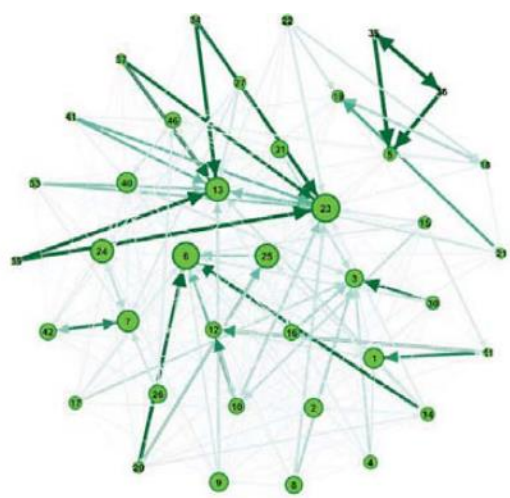


Figure 5 Relevance network diagram of lines in cascading failure.

Sequential Pattern Mining

[20] applies sequential pattern mining technology to cascading failure analysis and this existing works pay more attention to vulnerable lines and high-risk path, which are hard to explain the overall propagation characteristic of cascading failure. In figure 5, The edge with higher correlation index is wider and darker. According to graph theory, nodes with high degree play important roles in the cascading failure propagation process, such as Line L_{23}, L_6, and L_{25}

[21]uses the maximum flow analysis to investigate how targeted or random attacks on components of a power grid can affect the performance of the entire grid. The attacks are simulated by removing nodes or transmission lines from the network.

Reference	**Order** N	**Size** M	**ND**	B	**Attack strategy**	**w/u?**	**Electrical concepts into the CN approach**	**Metrics/indicators used in vulnerability analysis**
[17]	SN	SN	◇	◇	NA	**u**	–	ℓ, G
[141]	4941	–	◇	◇	NA	**u**	–	ℓ, G
[147]	14100	19660	◇	◇	NA	**u**	–	ℓ, Connectivity loss
[145]	14100	19660	◇	◇	NA	**u**	–	ℓ, E
[150]	3000	12000	◇	◇	NA	**u**	–	ℓ, G
[20]	3000	3800	◇		NA	**u**	–	ℓ, G
[19]	3000	3800	◇		NA	**u**	–	ℓ, G, ENS, TLP
[111]	4800	5500	◇		NA	**u**	–	$\ell, \mathcal{C}, G$
[152]	380	570			NA, LA	**u**	–	D
[154]	6400	8700			NA	**u**	–	$\ell, \mathcal{C}$
[155]	370	570	◇		LA	**u**	–	$\ell, \mathcal{C}$
[147]	14000	19600	◇	◇	NA	**u**	–	Connectivity loss
[151]	31400	–	◇		NA, EA	**u**	–	Probability of load loss
[156]	2700	3300	◇		NA	**u**	–	Motifs (sub-graph) size ENS, TPL, RT
[84]	8500	13900	◇		NA	**u**	–	G
[159]	4900	6600			NA	**u**	–	S_N
[107]	940	1260			NA	**u**	–	Blackout size
[149]	4940	6600	◇	◇	NA	**u**	–	G
[117]	4850	5300	◇	◇	NA	both	–	ℓ, G
[148]	340	520	◇	◇	NA	w	–	E
[153]	14000	19600			NA	w	–	E, D
[35]	550	700			NA	w	Impedance, DC flow	$E, \mathcal{A}$, overload
[85]	32	420			NA, LA	w	Impedance, DC flow	$\mathcal{B}_E$, ENS
[188]	90	120			LA	w	Impedance, DC flow	$E, \mathcal{A}$
[169]	200	400		◇	LA	w	Line impedance, DC flow	Overload, cascade
[87]	2930	6570		◇	NA	w	Line impedance, DC power flow	C_D^E
[173]	29500	50000			NA	w	Line impedance and DC flow	ℓ, connectivity level
[172]	550	800		◇	NA	w	DC flow	Connectivity, TLP
[7]	210	320		◇	NA	both	DC and AC power flow	Blackout size, $\mathcal{C}, \ell$
[174]	900	1150	◇	◇	NA	w	Line reactance	Loss of load, ℓ
[15]	570	870	◇	◇	NA	w	Active, reactive power loads	Loss of load
[175]	SN	SN	◇	◇	NA	w	AC model	$\overline{v}, S$, LD
[170]	2560	2890			NA, LA	w	Impedance	Largest power supply region
[181]	300	410	◇		NA	both	Line impedance	Impedance matrix sensitivity
[184]	150	46			NA	w	Line reactance, active power	E
[171]	39	46			NA	w	Line admittance, power flow	Flow availability
[30]	240	310			NA, LA	w	AC power flow model	C_D^E, C_B^E, ENS

Figure 6 Comparative study of selected references according to the metrics and indicators. "_" indicates that a metric is used. SN stands for several networks. "–" means not available/not used.

[16] analyze synthetic topologies as key study cases, such as IEEE bus networks, or WS networks, BA and ER networks, these latter being appropriate structures either to study asymptotic behaviors or to simplify the studies as shown in Figure6. The acronyms and symbols on the first row of this table are as follows: N (order, second column) and M (size, third column) are approximations, typically in the order

of tens, with the aim of giving a rough idea of order and the size of the network without getting lost in unnecessary details. ND and B stand for node degree analysis and betweenness statistic analysis, respectively. “AT” stands for attack strategy. “w/u?” denote whether weighted or unweighted links have been used in the graph that models the network. Finally, the last column represents the metrics that the surveyed works have used to study the vulnerability of the grid. Figure 7 is a Summarize of metrics and their corresponding equations, references and approaches in relation to figure6.

Metric	Equation or definition	Reference
Average path length, ℓ	(4)	[61]
Clustering coefficient, $\mathcal{C}$	(5)	[57]
Size of the largest connected component, G	(6)	[61]
Efficiency, E (definition 1)	(7)	[140]
Network Efficiency, E (definition 2)	(13)	[153]
Betweenness centrality, $C_B(v) \equiv \mathcal{B}_v$	(9)	[61]
Degree centrality, C_D	(10)	[30]
Damage, D	(14)	[153]
Normalized avalanche size, S_N	(15)	[162]
Geodesic vulnerability, $\overline{v}$	(20)	[175]
Impact on connectivity, S	(21)	[175]
Connectivity loss	Average decrease in the number of generators connected to a distributing substation	[153]
Connectivity level	Average fraction of generators connected by each load substation	[153]
Backup capacity, P_B	Additional link capacity (overcapacity) that needs to be supplied to secure the proper network operation when the most loaded link suffers from a failure or attack	[21]
Load shedding, LS	(22)	[175]
Electrical centrality, c_a	(23)	[173,181]
Electrical distance, **D**	(25)	[182,183]
Electrical degree centrality (def. 1), $C_D^E(i)$	(26)	[115,118,119,186]
Electrical degree centrality (def. 2), $C_D^E(i)$	(28)	[87]
Electrical betweenness centrality, $C_B^E(i)$	(27)	[34,115]
Electrical betweenness, $\mathcal{B}_E$	(30)	[8,78,85,168]
Net-ability, $\mathcal{A}$	(32)	[8,78,168]
Entropic degree, S_i	(34)	[8,78,168]
Effective graph resistance, R_G	(29)	[5,187]

Figure 7 Summary of metrics and their corresponding equations, references and approaches in relation to figure6

Marks :

[14]

Consumer Nodes (Loads) :

A consumer node dissipates power, and at the circuit level, it sinks current .

Distribution Nodes :

A distribution node is a connecting node that nether produces nor consumes power.

Generation Nodes :

A generation node is a fixed voltage source. The current emerging from this node depends on its own voltage, the power consumption of other nodes and the network topology.

Transformer Nodes :

Transformer nodes connect the high-voltage grids with mid-voltage or low-voltage grids.

[19]

Generation nodes:

These nodes are connected to generators via transformers in real power grid. They are the sources of electric energy.
Distribution nodes:
No generators are connected to such nodes, and in the topological structure each node is connected to only one single edge. Electricity is sent to consumers from such distribution nodes through low voltage transmission lines.
Transmission nodes:
No generators are connected to such nodes either, but in the topological structure each node is connected to more than one edge.

Reference

[1] Self-organized criticality and cascading failures in the topological model of power grids: a case study Carlotto, Tomas & Grzybowski, J.M.V.. (2014). Self-organized criticality and cascading failures in the topological model of power grids: a case study. 10.5540/03.2014.002.01.0098.

[2] Crucitti, Paolo , V. Latora , and M. Marchiori . "A model for cascading failures in complex networks." *Physical Review E Statistical Nonlinear & Soft Matter Physics* 69.4 Pt 2(2003):045104.

[3] A. Kyriacou, P. Demetriou, C. Panayiotou and E. Kyriakides, "Controlled Islanding Solution for Large-Scale Power Systems," in IEEE Transactions on Power Systems, vol. PP, no. 99, pp. 1-1.

[4] Pahwa, Sakshi & Hodges, A & Scoglio, Caterina & Wood, Sean. (2010). Topological analysis of the power grid and mitigation strategies against cascading failures. 272 - 276. 10.1109/SYSTEMS.2010.5482329.

[5] Soltan, Saleh, D. Mazauric, and G. Zussman. "Cascading Failures in Power Grids - Analysis and Algorithms." Computer Science (2014):195-206.

[6] J. Yan, Y. Tang, H. He and Y. Sun, "Cascading Failure Analysis with DC Power Flow Model and Transient Stability Analysis," in IEEE Transactions on Power Systems, vol. 30, no. 1, pp. 285-297, Jan. 2015.

[7] Ko, Yakup, et al. "The impact of the topology on cascading failures in a power grid model." Physica A: Statistical Mechanics and its Applications 402(2014):169-179.

[8] https://en.wikipedia.org/wiki/Cascading_failure

[9] Xiaohui, Ye , et al. "Review on power system cascading failure thoeries and studies." *International Conference on Probabilistic Methods Applied to Power Systems* IEEE, 2016.

[10] Cascading Failure Analysis Considering Interaction Between Power Grids and Communication Networks

[11] R. Zimmerman, C. Murillo-Sánchez, and R. Thomas, “MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education,” *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[12] Song, Jiajia , et al. "Dynamic Modeling of Cascading Failure in Power Systems." *IEEE Transactions on Power Systems* (2014).

[13] Zhang X, Zhan C, Tse CK. Modeling the dynamics of cascading failures in power systems. IEEE J Emerg Sel Top Circuits Syst 2017 3.

[14] Zhang X, Tse CK. Assessment of robustness of power systems from a network perspective. IEEE J Emerg Sel Top Circuits Syst 2015;5:456–64. http://dx.doi.org/10.1109/JETCAS.2015.2462152.

[15] Sch?Fer, Benjamin , et al. "Dynamically induced cascading failures in power grids." *Nature Communications* 9.1(2018):1975.

[16] Cuadra, et al. "Energies, Vol. 8, Pages 9211-9265: A Critical Review of Robustness in Power Grids Using Complex Networks Concepts." (2015).

[17] Bompard, Ettore , D. Wu , and F. Xue . "Structural vulnerability of power systems: A topological approach." *Electric Power Systems Research* 81.7(2011):1334-1340.

[18] Bompard, E. , R. Napoli , and F. Xue . "Extended topological approach for the assessment of structural vulnerability in transmission networks." *IET Generation, Transmission & Distribution* 4.6(2010):1.

[19] Han, Pingping and Sixun Zhang. “Analysis of Cascading Failures in Small-world Power Grid.” (2011).

[20]

[21] Atkins, Karla & Chen, Jiangzhuo & Kumar, Sritesh & Marathe, Achla. (2009). The structure of electrical networks: A graph theory based analysis. IJCIS. 5. 265-284. 10.1504/IJCIS.2009.024874.